Washington Meetings Program and the Digital and Cyberspace Policy Program:

A Conversation with Giovanni Buttarelli

Council on Foreign Relations, Washington DC, 10 March 2015, 8:30-9.30am

Ladies and gentlemen,

I'm very grateful to the Council on Foreign Relations and the Digital and Cyber Policy Program for this opportunity to talk with you this morning.

It's a great opportunity because, all of a sudden, privacy and personal data have become a 'Big Deal'.

The fact that we are here in Washington DC, at this time, to discuss this theme, is testimony to how privacy has climbed up the scale of issues strategic importance.

So much so, in fact, that this expert gathering has invited a privacy regulator from Europe.

Not so long ago data protection was largely the preserve of specialist legal academics and human rights campaigners.

Now it's headline news – 'the right to be forgotten', Facebook buying What's App for $22bn, the Sony hack, the steady drip-drip-drip of revelations about mass scale surveillance by security agencies - these stories now matter to chief economists, CEOs, Government ministers and security chiefs.

Lawmakers are responding now. The White House has just published its long awaited draft Consumer Privacy Bill of Rights Act. Japan and Brazil are considering reforming its data rules. And of course the European Union as well as the Council of Europe are at advanced stages in reform of their respective data protection frameworks.

The tectonic plates of data laws are shifting, and in many ways Europe is at the epicentre of this realignment. In the next 10 minutes I'm going to try to explain why...

I was appointed European Data Protection Supervisor in December 2014 with a five year mandate.

The role of EDPS is relatively new. The European Union established my office just over a decade ago, as part of a wider framework governing how European institutions should themselves apply high standards in how we handle personal information.

My function is to supervise and to advise. I have, together with my good colleague Assistant EDPS Wojciech Wiewiórowski a small staff of around 50, lawyers, administrators and IT specialists. Together we enforce compliance by large scale IT systems and around 70 separate European institutions and bodies with data protection rules.

But we are also active in policymaking. And policymaking in Brussels is a daunting ordeal, even for old hands like myself.

To summarise the process:

- Pressure for regulation builds steadily, eventually the Commission take up the challenge of drafting a law which generally attempts to please all parties a little, though seldom pleasing any of them very much.
- Then it passes to one or more committees (depending on its scope and complexity) of the European Parliament, and to one or more working groups of the Council, which brings together national governments of the 28 Member States.

Many of these initiatives, an increasing number, involve handling personal information or have an impact on privacy.

My institution tries to inform and to steer the lawmakers towards conclusions which are good for the individual, their rights and interests, but also for public bodies and businesses.

One of the biggest issues for the last three years has been data protection reform.

Social, technological and political developments have generated a perfect storm, consisting of calls for change.

We are just beginning to realise the sheer transformative power of the internet and communication technology, whether it's reconnecting lost school friends to the potential for containing epidemics and reducing road accidents.

Fibre-optic cables can now transmit in 20 seconds data equivalent to the entire printed collection of the Library of Congress.

Big data is often personal information, and it carries with it value, knowledge and power.

We know this from our recent work in stimulating a debate, on both sides of the Atlantic, with the European Commission and the Federal Trade Commission, on whether antitrust rules are robust enough to ensure full and fair competition in the digital economy.

Meanwhile, the Snowden revelations rocked trust in government and caused citizens in Europe and the US to question the effectiveness of the democratic constraints and accountability of those who are meant to protect us from harm.

The current data protection framework in the EU is 20 years old this year. That's 20 years ago:

- when the internet was in its infancy,
- when barely 100m desktops were being shipped per year,
- when mobile phones penetrated only about 10% of the population the US and Western Europe.

The guiding principles of the EU's Data Protection Directive are, in my view, as sound today as they were back in 1995:

- that information relating to an individual must be treated fairly,
- for specific purposes,
- on the basis of consent by the individual or one of several other valid legal bases,
- the individual's right to have access to data collected about him or her,
- that there must be an authority independent of government to ensure compliance.

Indeed these principles a few years later in 2001 became codified in the EU's Charter of Fundamental Rights. That document now has the equivalent status in the EU as the Constitution here in the US.

But there is a consensus that the rulebook needs an upgrade.

The European Commission's 2012 proposal for a General Data Protection Regulation was ambitious and far reaching. It will affect everyone in the world who processes personal data affecting individuals in the EU for commercial purposes, for purposes of public administration, any purpose which is not a purely 'personal or household' activity.

Whereas the 1995 directive has to be implemented through various national transposing laws, the Commission's proposed regulation would apply directly to all data controllers.

The proposal is detailed – some say, and I have some sympathy with this view with regard to specific provisions – too detailed: setting out the obligations those who are responsible for data processing and those who process on behalf of the person or organisation who is responsible.

And, unlike the 1995 directive, the new regulation will have real teeth. Fines for breaches of rules could be up to 5% of the annual worldwide turnover in case of an enterprise, according to the Parliament's revision of the Commission's proposal.

That's why this reform is sending shock waves around board rooms around world. That's why a record 4000 amendments were tabled.

More than ever before there is a need for objective, informed and impartial advice on how to find a way though this minefield.

On Monday, just under 90 days into my mandate, I published a strategy for how my office intends to meet this challenge. The short document, which I would humbly

encourage you to read, is based on three main objectives and 10 specific actions. I will briefly summarise them.

First, let's take data protection digital.

We need to find new ways for applying data protection principles to the latest technologies, be it big data, the internet of things, cloud computing, artificial intelligence, drones or robotics. We need to place the individual more firmly at the heart of technological development, through transparency, user control and accountability.

By way of illustration, much newsprint has been devoted to the so called 'new right to be forgotten'. In fact, this expression is catchy but also perhaps misleading.

In its judgment on Google Spain in May last year, the European Court of Justice did not invent a new right. It rather confirmed that if you process personal data (and, it ruled, search engines certainly do process and make decisions on processing personal data) then you have a responsibility to treat those data in a way that respects the rights and interests of the individual. Part of that responsibility is enabling the individual to challenge what you do with the information which relates to him or her.

In the headlong rush for innovation, we cannot forget the human element – that was the message of Stephen Hawking and the Future of Life Institute in their open letter in January – and I see our strategy as a challenge to the EU to respond that call.

Second, we need global partnerships on the big questions posed by these technologies, and by the social and economic changes which accompany them. Big data will need equally big data protection. I believe in interoperability– a fashionable term, and a fashionably vague term – between different approaches to privacy and data protection, if such interoperability is genuinely two-way, and both sides in the discussion respect the other's values in practice, not just in words.

This must be borne in mind for agreements like Safe Harbor, for security cooperation, and in trade negotiations. Bilateral agreements even with our closest strategic partners cannot be a back door for weakening the protection of the rights for which generations have fought.

Third, we need a new deal on data protection in the EU and we need it fast. The new data protection regulation is just the beginning: we need to mainstream the rights of the individual throughout all policies, whether on law and order, financial services regulation, exchange of health data, or competition and consumer law.

On each of these fronts the EDPS will engage proactively and honestly. And we will broaden the debate beyond politicians, privacy lawyers and regulators.

So, in conclusion, I hope I've begun to persuade you that we are indeed witnessing a tectonic shift in how society responds to technological innovation.

'New deal' is another a cliché – Europeans love to plagiarise the American lexicon for their own ends. But it's deeply resonant, reminding us of Roosevelt's policies for regenerating a depressed economy.

Europe by common consent needs a kick start. There is a real risk of torpor and stagnation – I need only cite the drift to negative interest rates, the rise of populist parties and declining voter turnout in elections.

Personal data regulation has a strategic importance for rebuilding trust between government and citizens, big business and consumers, between the EU and the US.

EDPS strategy focuses on how to find pragmatic solutions to shape, not slow, technological development and laws in the interests of the individual.

We do not need to reinvent data protection principles, but we do need to '*go digital*', to make them more effective in practice in our technology-driven society, and to integrate them with some new principles specifically arising from the digital age.

Data protection is too important to be simply the subject of arid debates between privacy lawyers and regulators. This is why we want to better explore the ethics of these changes.

The EU and the US has strong cultural, economic and strategic ties – so we must seize the opportunity to build some consensus: towards a new deal on transatlantic data flows. A digital deal.

- - - - - -